

AFFIDAVIT

I, Amy L. Ramsey, Special Agent of the Federal Bureau of Investigation ("FBI"), Kansas City, being duly sworn, hereby state as follows:

1. I am a Special Agent of the FBI assigned to the Kansas City Division of the FBI. I have been continuously employed by the FBI since November of 2003, including previous assignments to the Boston and New York Divisions. Since arriving in the Kansas City Division of the FBI in August of 2012, I have been assigned to investigate criminal enterprises. As a Special Agent of the FBI, I am empowered to conduct investigations of, and to make arrests for, offenses related to the Interstate Transportation of Stolen Property enumerated in Title 18 of the United States Code.

2. While with the FBI, I have participated in numerous investigations targeting criminal organizations and enterprises. I have actively investigated organizations involved in the interstate transportation of stolen property, unlawful possession and distribution of controlled substances, organizations that perpetrate fraudulent schemes as a means of producing income for the enterprise, as well as investigations directed at monetary transactions involving the proceeds of specified unlawful activities and conspiracies. My training and experience has involved wire and electronic surveillance, physical surveillance, execution of search warrants, execution of criminal arrests and the handling of cooperating sources and other sources of information.

3. On numerous occasions, I have spoken with subjects, defendants, and other investigators concerning the methods and practices of criminal organizations. Through these investigations, my training, experience, conversations with experienced agents, investigators, and

law enforcement personnel, in the United States and elsewhere, I have become familiar with the general methods employed by traffickers of stolen property. These methods include wireless communications technology such as cellular telephones, counter surveillance, false or fictitious identities, and the use of coded communications in an attempt to avoid detection by law enforcement and circumvent investigations. Based on my training and experience, I am familiar with methods used to obtain, distribute, and sell stolen property, as well as methods used to conceal the sources of the illicit funds received from the sales of said stolen property.

4. This Affidavit is in support of a search warrant for an Apple iPhone Xs Max cellular telephone, Model Number MT652LL/A, Serial Number FFWXN72XKPHC, IMEI number 357274099815714 (“**TARGET TELEPHONE 1**”) and a rose gold Apple iPhone cellular telephone encased in a black Otter Box, bearing unknown serial number (“**TARGET TELEPHONE 2**”), for violations of Title 18, United States Code, Section 2314, Interstate Transportation of Stolen Goods. Subscriber information from T-Mobile revealed **TARGET TELEPHONE 1** to be subscribed by Danielle Jackson, known associate and girlfriend of subject Viktor Chernetskiy. Chernetskiy is believed by law enforcement to be the sole user of **TARGET TELEPHONE 1**.

5. On May 24, 2019, United States Magistrate Judge Lajuana M. Counts, Western District of Missouri, signed a court order, Case No. 19-SW-00164-LMC, authorizing the installation of Global Positioning System (“GPS”) tracking on cellular telephone number (816) 258-2499 (i.e., **TARGET TELEPHONE 1**), known to be used by Chernetskiy.

6. On June 13, 2019, around 6:54 p.m., I became aware that **TARGET TELEPHONE 1**, used by Viktor Chernetskiy, was traveling southbound on Interstate 35, in the vicinity of Lebo, Kansas. I was able to then review previous **TARGET TELEPHONE 1**’s

location “pings” to determine that **TARGET TELEPHONE 1** was in the vicinity of 11008 Grandview Road, Kansas City, Missouri, around 5:06 p.m. At the time of the next ping location for **TARGET TELEPHONE 1**, approximately 5:37 p.m., **TARGET TELEPHONE 1** appeared to be moving westbound along the vicinity of I-435. With these times of **TARGET TELEPHONE 1**’s movements, I was able to review surveillance footage that showed a silver Dodge Charger, previously identified as having Missouri license plate D5262-AE, arriving at the residence at 11008 Grandview around 5:28 p.m. At that time, an adult wearing gray pants and a dark colored shirt appeared to walk around the Charger before re-entering the passenger side of the car, which departed 11008 Grandview around 5:33 p.m.

7. Upon observing the **TARGET TELEPHONE 1**’s location to be approaching Lebo, Kansas, investigators determined a physical surveillance of the vehicle would not be possible during its southbound travel, due to it having departed well in advance of the investigators. I, along with other investigators, monitored the location of **TARGET TELEPHONE 1** via the previously authorized GPS tracking of the phone. By approximately 8:24 p.m., **TARGET TELEPHONE 1** appeared to be westbound on U.S. 400 Highway, west of Wichita, Kansas. Around 9:23 p.m., investigators received information that the silver Charger, bearing Missouri license plate D5262-AE, had been captured via a license plate reader along I-35 southbound, south of Emporia, Kansas, around 7:08 p.m., confirming the movement of **TARGET TELEPHONE 1** along with the silver Charger. Around 10:06 p.m., **TARGET TELEPHONE 1** appeared to be southbound on Highway 281, in Oklahoma.

8. Around 3:07 a.m. on June 14, 2019, Special Agent McKune observed a GPS location for **TARGET TELEPHONE 1** in the vicinity of Enid, Oklahoma. In the early morning hours of June 14, 2019, Missouri State Highway Patrol (“MSHP”) Master Sergeant Brad Ream

obtained information from the Enid, Oklahoma Police Department that a burglary had occurred at the Pioneer Telephone Cooperative, Inc, Store, located in Enid, Oklahoma, around 2:50 a.m. on June 14, 2019. Enid, Oklahoma Police Department provided photographs of a silver Dodge Charger captured from security cameras at the store. Further, Enid, Oklahoma Police provided color photographs captured of two subjects within the Pioneer Store that appeared to show them loading cellular telephone boxes into a black plastic trash bag.

9. The first male shown in the photographs obtained from Enid, Oklahoma Police Department appeared to be a heavy-set male with gray pants and a gray hooded sweatshirt. The hood of the sweatshirt was drawn tightly around a baseball cap with a flat shaped, gray bill, with a round black and silver sticker on the top of the bill. The individual also appeared to be wearing black Nike shoes with a gray tongue and/or laces, yellow work gloves, and appeared to be holding an orange screw driver or tool of some sort. At the time that a traffic stop was conducted on the Dodge Charger by MSHP around 7:50 a.m., on June 14, 2019, near Red Bridge Road and Highway 71 in Kansas City, Missouri, Viktor Chernetskiy was wearing a gray sweat suit with a hooded shirt and a black “Spurs” hat with a gray bill and a shiny, round, sticker on the flat shaped bill. Chernetskiy was also wearing black Nike shoes with a gray tongue and/or laces.

10. The second male shown in the photographs obtained from Enid, Oklahoma Police Department appeared to be a slender male wearing a black bodied hooded sweatshirt with gray sleeves, with the hood drawn tightly around his head. He also wore what appeared to be dark colored Nike shoes, and possibly white gloves as he held the black plastic bag open for the heavy-set male to place phones into it. At the time that a traffic stop was conducted on the Dodge Charger by MSHP around 7:50 a.m., on June 14, 2019, near Red Bridge Road and Highway 71 in Kansas City, Missouri, Bryan Kirkendoll was observed to be wearing a black

bodied, hooded sweatshirt with gray sleeves, and light gray pants, consistent with those observed in the photos provided by Enid, Oklahoma Police Department.

11. Enid, Oklahoma Police Department advised that approximately 157 cellular telephones were burglarized from the Pioneer Telephone Cooperative, Inc, in Enid, Oklahoma, with a total value of approximately \$147, 587.

12. Around 3:36 a.m., on June 14, 2019, Special Agent McKune observed a GPS location for **TARGET TELEPHONE 1** in the vicinity of Pond Creek, Oklahoma. In the early morning hours of June 14, 2019, MSHP Master Sergeant Brad Ream obtained information from the Pond Creek, Oklahoma Police Department that a burglary had occurred at the Pioneer Telephone Cooperative, Inc., Store, located in Pond Creek, Oklahoma, around 3:30 a.m., on June 14, 2019.

13. Pond Creek, Oklahoma Police Department advised that approximately 27 iPhones, one internet router, and one unknown item were burglarized from the Pioneer Telephone Cooperative, Inc., Store, located in Pond Creek, Oklahoma. Investigators have received photographs and security video from this store. The security video depicted two males matching the descriptions above moving through the store with their faces covered. Toward the end of the security video footage, I believe Kirkendoll, who carried a full black trash bag, moved toward the exit of the store with Chernetskiy trailing behind him. Security video footage from the exterior of the business depicted a silver Dodge Charger, that matched the description of Chernetskiy's known vehicle described above, driving in the vicinity of the store.

14. Around 4:40 a.m., on June 14, 2019, the silver Dodge Charger was captured via license plate reader entering Kansas along I-35 northbound. Around 6:30 a.m., Special Agent

McKune observed the silver Dodge Charger travelling northbound on I-35, at County Road U, east of Emporia, Kansas.

15. Around 7:05 a.m., on June 14, 2019, I observed the silver Dodge Charger to stop at the Loves Gas Station, located at 203 East 27th Street, Ottawa, Kansas. After getting gas, I observed Kirkendoll exit the store and enter passenger door of the Charger. At that time, Kirkendoll was observed to be wearing gray pants and dark hooded sweatshirt with a white Nike symbol on the front.

16. Special Agent McKune and I then maintained physical surveillance of the vehicle until MSHP was able to affect a traffic stop of the vehicle around 7:50 a.m., on June 14, 2019, near Red Bridge Road and Highway 71 in Kansas City, Missouri. At the time of the stop, the driver was identified as Viktor Chernetskiy and the passenger was identified as Bryan Kirkendoll. The location of where MSHP stopped Chernetskiy and Kirkendoll was in close proximity to the residence at 1108 Grandview Road, Kansas City, Missouri. It is believed by law enforcement that Chernetskiy was returning to the residence at the time of the stop.

17. At the time of the above-mentioned traffic stop, the silver Dodge Charger was seized for evidence by MSHP and transported by tow truck to MSHP Troop A Headquarters in Lee's Summit, Jackson County, Missouri. The GPS "pings" from Chernetskiy's telephone continued to provide data corroborating the location of the cellular telephone with the Dodge Charger. At the time of their detention, neither Chernetskiy nor Kirkendoll had cellular telephones on their persons. Law enforcement believed the phones remained inside of the vehicle at the time of the seizure.

18. On June 14, 2019, a criminal complaint was filed in the Western District of Missouri charging Chernetskiy and Kirkendoll with aiding abetting the interstate transportation

of stolen property, in violation of Title 18, United States Code, Sections 2314 and 2. On that same day, Chernetskiy and Kirkendoll were arrested pursuant to a federal arrest warrant.

19. On June 14, 2019, United States Magistrate Judge Lajuana M. Counts, Western District of Missouri, in Case Number 19-SW-00198-LMC, issued a search warrant for the silver Dodge Charger. The search warrant was executed on June 17, 2019. At the conclusion of the search a total of 183 stolen Apple iPhones were seized from the rear compartments of the vehicle, physical items related to how the burglaries were conducted, as well as two used Apple iPhones located in the front compartment of the vehicle. One of the used Apple iPhones, identified as **TARGET TELEPHONE 1**, was turned on and connected to a charging port next to the driver's seat. It is known by law enforcement that Chernetskiy was driving the vehicle at the time of his initial arrest. Upon seizing **TARGET TELEPHONE 1**, a photograph of Chernetskiy was observed as the background of the device.

20. By way of background into the initiation of the above investigation, law enforcement has maintained evidence against Chernetskiy from multiple burglaries of cellular telephone stores in the states of Kansas, Missouri, and Iowa, in addition to the two described above in Oklahoma, between December 2018 and June of 2019. One such piece of the evidence is surveillance footage where law enforcement believes Chernetskiy worked with other unknown individuals to burglarize the stores. Through training and experience, I know that criminal organizations utilize cellular telephones to communicate with one another.

21. In May 2019, during an in person contact with MSHP Master Sergeant Ream, Chernetskiy provided the **TARGET TELEPHONE 1** number as his current cellular telephone device.

22. During the search of the Dodge Charger on June 17, 2019, the only other unpackaged and used cellular telephone in the vehicle, known here as **TARGET TELEPHONE 2**, is believed by law enforcement to belong to Chernetskiy's co-conspirator Bryan Kirkendoll.

23. Based upon my training and experience in criminal enterprise investigations, I am aware that cellular telephones are a tool that are regularly used by those engaging in the trafficking of stolen goods. Co-conspirators often call each other to arrange places and times to meet, as well as discuss target locations for criminal activity. Co-conspirators also sometimes send text messages to each other to arrange places and times to meet, as well as to discuss target locations for criminal activity. I am aware that cellular telephones maintain call logs of recent incoming and outgoing telephone calls, which often include contacts with other co-conspirators. I am aware that cellular telephones save the text messages sent and received. I am also aware that co-conspirators often add the phone numbers of other co-conspirators into their "contacts" list in their cell phones, providing monikers or other evidence of who the other co-conspirators might be. I am aware that certain telephones also have capabilities to make notes, keep calendars, and various other functions; all of which might provide additional information regarding the alleged crime of possession with intent to distribute controlled substances. As such, I believe that **TARGET TELEPHONE 1** and **TARGET TELEPHONE 2**, both having been seized from the Dodge Charger on June 17, 2019, and currently maintained in the custody of the FBI, are likely to contain evidence of the criminal activity described above.

24. I know through the investigation that Chernetskiy has traveled long distances to commit the above-mentioned burglaries of cellular telephone stores and I understand that when individuals travel to unfamiliar locations a GPS is typically used to aid in the navigation process. No other GPS was located in the vicinity of the Dodge Charger leading investigators to believe

that a log of **TARGET TELEPHONE 1**'s locations will be maintained in the device, providing further evidence of the burglaries.

25. Your Affiant further affirms that three identified associates and suspected co-conspirators, attempted to contact **TARGET TELEPHONE 1** during the search of the vehicle. When cellular telephones receive notifications, the face of the device will light up in response. During the course of the vehicle search on June 17, 2019, law enforcement observed the face of **TARGET TELEPHONE 1** light up with several notifications to include the three suspected co-conspirators.

26. On June 18, 2019, during an interview of a cooperating witness who employed Chernetskiy in May and June 2019, a contract between the employer and Chernetskiy was provided to investigators. Chernetskiy's signature was observed on the contract and next to his signature was a written telephone number, identified as (816) 258-2499, also known as the telephone number assigned to **TARGET TELEPHONE 1**.

27. **TARGET TELEPHONES 1 and 2** have been maintained by the FBI's Kansas City Division, Evidence Control Unit at 1300 Summit Street, Kansas City, Jackson County, Western District of Missouri. In my training and experience, I know that the **TARGET TELEPHONES 1 and 2** have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the cellular telephones first came into the possession of the FBI.

TECHNICAL TERMS

27. Based on my training and experience, I use the following technical terms to convey the following meanings: Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless, device used for voice and data communication through

radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.

28. Based on my training, experience, and research, I know that cellular telephones have capabilities that allow it to serve as a wireless telephone, digital camera, and GPS navigation device. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device, and the location of the device’s usage.

29. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. *Forensic evidence.* This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the listed cellular telephones were used,

the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the listed cellular telephones because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, where the usage occurred, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, where it was used, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.
- f. Information stored within a cellular phone (cell phone) may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored within a cell phone can indicate who has used or controlled the cell phone. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, contacts lists, instant messaging logs, and communications (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the cell phone at a relevant time. Further, such stored electronic data can show how and when the cell phone and its related account were accessed or used. Such “timeline” information allows investigators to understand the chronological context of cell phone access, use, and events relating to the crime under investigation. This “timeline”

information may tend to either inculcate or exculpate the cell phone account owner. Additionally, information stored within a cell phone may indicate the geographic location of the cell phone and user at a particular time (e.g., location integrated into an image or video sent via email or text message to include both metadata and the physical location displayed in an image or video). Last, stored electronic data may provide relevant insight into the cell phone owner's state of mind as it relates to the offense under investigation. For example, information in the cell phone may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement). Unless this data is destroyed, by breaking the cell phone itself or by a program that deletes or over-writes the data contained within the cell phone, such data will remain stored within the cell phone indefinitely.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

32. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

- a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;
- b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);
- c. Surveying various file directories and the individual files they contain;

- d. Opening files in order to determine their contents;
- e. Scanning storage areas;
- f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described above in paragraph 4 of this Affidavit; and/or
- g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described above in paragraph 4 of the Affidavit.


Manner of execution.

- a. Computer storage devices, (like modern day cellular phones, SIM cards and micro cards, hard disks, diskettes, tapes, laser disks, Bernoulli drives) can store the equivalent of hundreds of thousands of pages of information. Additionally, a suspect may try to conceal criminal evidence, and he or she might store criminal evidence in random order with deceptive file names. This may require searching authorities to examine all the stored data to determine which particular files are evidence or instrumentalities of crimes related to violations of 18 U.S.C. § 2423. After the initial imaging, the examiner and agents will not further save or copy data unrelated to those violations. To the extent possible, they will minimize the review of unrelated data. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this kind of data search on site.
- b. Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is good cause for the Court to authorize execution of the warrant at any time in the day or night.

VI. CONCLUSION

33. Based upon the foregoing, my training and experience, and through the evidence gathered in the course of this investigation, I believe there is probable cause that the listed digital devices, and any incorporated SIM card and/or micro card contain documents, photographs, text messages, direct messages, internet history, e-mails, "address books" or "contacts" lists, call logs, audio files, and other types of electronic media, that constitutes evidence and/or fruits and

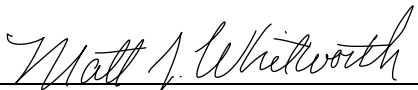
instrumentalities of criminal offenses, including violations of 18 U.S.C. § 2314, Interstate Transportation of Stolen Goods. I submit that this Affidavit supports probable cause for a search warrant authorizing the examination of the digital device described above in paragraph 4 of this Affidavit, for the items listed in Attachment A.



AMY L. RAMSEY
Special Agent
Federal Bureau of Investigation

Sworn and subscribed before me

this 21st day of June, 2019.



HONORABLE MATT J. WHITWORTH
Chief United States Magistrate Judge
Western District of Missouri